ملخص

شبكة الاستشعار اللاسلكية تتزايد أهميتها وهذا نظرا لتواجدها في العديد من المجالات منها: العسكري والطبي ...إلخ، تلك التطبيقات تتطلب مستوى عالي من الأمن نظرا لحساسية هذه المجالات. في عملنا هذا نقدم مجموعة من خوارزميات التشفير المهمة. هدفنا الرئيسي هو استعمال وتطبيق هذه الخوارزميات في جهاز الاستشعار لتقييم أدائها بشأن استهلاك الطاقة، والتخزين في الذاكرة ووقت التنفيذ. نتائجنا تعتمد على استخدام نوعين مختلفين من أجهزة المحاكاة TOSSIM وAVRORA.

الكلمات المفتاحية: شبكة الاستشعار اللاسلكية،خوارزميات التشفير،TOSSIM ،AVRORA.

Résumé

Les réseaux de capteurs sans fil (RCSF) sont de plus en plus importants du fait qu'ils sont présents dans de nombreuses applications telles que : militaires, médicales…etc. Ces applications ont souvent besoin d'un niveau de sécurité important. Dans ce mémoire, on présente un état de l'art des principales primitives cryptographiques. Notre objectif est de pouvoir implémenter des différentes primitives étudies dans un capteur pour évaluer ses performance en terme de consommation de l'énergie, occupation de l'espace de mémoire, et le temps d'exécution. Nos résultats expérimentaux sont basés sur l'utilisation de deux types des simulateurs : TOSSIM et Avrora.

Mots-clés : RCSF, primitives cryptographique, capteur, TOSSIM, Avrora.

Abstract

The wireless sensor networks (WSN) are growing more important that they exist in many applications such as: military, medical…etc. These applications require a high security level. In our work, we represent state of the art about cryptographic primitives. Our main objective is to implement different studied primitives in a sensor to evaluate its performance concerning the energy consumption, the occupied storage and the execution time. Our results based on using two different types of simulators: TOSSIM and Avrora.

Keywords: WSN, cryptographic primitives, TOSSIM, Avrora.